UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	**TO BE FILED UNDER SEAL**
	:	
v.	:	Hon. Cathy L. Waldor
	:	
MAKSIM BOIKO a/k/a "GANGASS"	:	Mag. No. 20-9121
	:	
	:	**CRIMINAL COMPLAINT**

I, Kevin M. Conklin, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this Complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.

KMC (by phone)
Kevin M. Conklin, Special Agent
Federal Bureau of Investigation

Special Agent Conklin attested to this Affidavit by telephone pursuant to FRCP 4.1(b)(2)(A)

March 27, 2020 at _____
District of New Jersey

HONORABLE CATHY L. WALDOR
UNITED STATES MAGISTRATE JUDGE

s/Cathy L. Waldor 3/27/20 by telephone
Signature of Judicial Officer

ATTACHMENT A

(Money Laundering Conspiracy)

From at least as early as on or about March 13, 2017 through at least on or about September 12, 2017, in the District of New Jersey and elsewhere, defendant

MAKSIM BOIKO,
a/k/a
"GANGASS,"

did knowingly combine, conspire, and agree with other individuals to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, wire fraud, knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, contrary to Title 18, United States Code, Sections 1956(a)(1)(B)(i).

In violation of Title 18, United States Code, Section 1956(h).

ATTACHMENT B

I, Kevin M. Conklin, being first duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been employed by the FBI as a Special Agent since February 2002. My experience as an FBI agent has included the investigation of cases involving money laundering, wire fraud, and the use of computers to commit such offenses. I have received training and have gained experience in interview and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures.

2. Since this Affidavit is submitted for the sole purpose of establishing probable cause to support the issuance of a federal criminal complaint and arrest warrant, I have not included each and every fact known by the Government concerning this investigation. Except as otherwise indicated, the actions, conversations, and statements of others identified in this Affidavit – even where they appear in quotations – are reported in substance and in part. Similarly, dates and times are approximations, and should be read as "on or about," "in or about," or "at or about" the date or time provided.

OVERVIEW

3. From at least as early as on or about March 13, 2017 through at least on or about September 12, 2017, individuals both known and unknown conspired to launder the proceeds of criminal activity, including Internet-enabled financial fraud.

INDIVIDUALS, ENTITIES, AND BANK ACCOUNTS

4. At various times relevant to this Complaint:

a. Defendant Maksim Boiko, a/k/a "Gangass" ("**BOIKO**") was a resident of Russia. BOIKO laundered criminal proceeds for cybercriminals. BOIKO communicated with other cybercriminals by using encrypted communication platforms that are designed to conceal correspondence. BOIKO was a member of Verified, a prominent cybercrime forum.

b. "**Person A**" was a resident of Russia. Person A was a cybercriminal who used various unidentified computer intrusion techniques to gain access to sensitive banking information from business and individual accounts. After he gained access to victim bank accounts, he coordinated unauthorized bank transfers from the victim accounts to accounts that he or his co-conspirators controlled. Person A further targeted victims with "flooding" attacks to facilitate the unauthorized bank transfers. Flooding attacks are a type

of "denial-of-service" attack in which actors overwhelm a victim's computer network or telephone line with a large volume of messages and/or calls, which hinders the victims' ability to respond to or disrupt a simultaneous cyber breach.

c. "**Victim A**" was a California business entity with a bank account at a U.S.-based financial institution ("**Financial Institution 1**"). Financial Institution 1 was a financial institution as defined under 18 U.S.C. § 1956(c)(6)(A) and 31 U.S.C. § 5312(a)(2).

d. The "**Destination Bank Account**" was a bank account at a financial institution in China ("**Financial Institution 2**.").

e. "**Victim B**" was a small business in Secaucus, New Jersey, that maintained a credit card account at a U.S.-based financial institution ("**Financial Institution 3**"). Financial Institution 3 was a financial institution as defined under 18 U.S.C. § 156(c)(6)(A) and 31 U.S.C. § 5312(a)(2). As an account holder, Victim B could electronically access information about its account through Financial Institution 3's password-protected online banking portal. Victim B participated in Financial Institution 3's customer loyalty rewards program, which allowed customers to earn "points" that could be redeemed for gift cards or other merchandise.

f. "**Victim C**" was a small business in Englewood Cliffs, New Jersey, which maintained a bank account at Financial Institution 1.

THE GOAL OF THE CONSPIRACY

5. The goal of the conspiracy was to facilitate the "cashing out" of criminal proceeds and to conceal from law enforcement and financial institutions the criminal nature of the funds.

MANNER AND MEANS

6. On or about March 10, 2017, on the "Jabber" chat platform,[1] Person A asked another individual ("**Individual 1**") to be put in communication with someone who could provide bank accounts and who could "cash out" funds. Specifically, Person A stated: "[L]et this cashout guy contact me . . . hk/cn . . . because we need accounts sometimes . . . it is better to have direct communication."[2] Based on my training and experience, "hk/cn" refers to Hong

[1] "Jabber" is a protocol for creating real-time, text-based chat software, and it allows users to create their own chat service hosted on computers that they choose. Jabber account addresses look similar to email addresses with an account identifier preceding the "@" symbol, followed by a domain address associated with the Jabber server. Because Jabber accounts can be created and hosted by cybercriminals themselves, it is often a favored method of communication for cybercriminals.

[2] The electronic communications reviewed in this Complaint took place in Russian, and have been translated into English by the FBI. All translations are approximate.

Kong and China, which are common destinations for funds obtained through Internet-enabled fraud. In response, Individual 1 gave Person A contact information for BOIKO. On or about March 13, 2017, Person A told another associate, "I found a guy . . . hk/cn cashout is his."

7. On or about March 13, 2017, BOIKO and Person A communicated via Jabber. BOIKO stated, "hi, here." Person A responded: "hi . . . write with otr." Based on my training and experience, "otr" means "off the record," and "write with otr" is an instruction to switch over to encrypted communication, so that the communication would later be more difficult for law enforcement authorities to review. On or about March 14, 2017, and March 16, 2017, BOIKO and Person A communicated again via encrypted messaging on Jabber.

8. On or about March 20, 2017, at approximately 19:00 Coordinated Universal Time (UTC), Person A asked BOIKO to quickly provide him with bank account information. He stated, "hi urgent . . . what is going on with business accounts . . . hurry up pls time is limited." In response, at approximately 19:02 UTC, BOIKO stated that he already provided an account to Person A. Person A recited information regarding a bank account, and BOIKO stated that that was a "personal account." At approximately 19:03 UTC, Person A replied: "give me business pls . . . can you do it now . . . I only have 5-10 min." Based on my training and experience, compared to personal bank accounts, business bank accounts are able to receive larger sums of stolen funds without raising the suspicion of bank officials. Additionally, based on my training and experience, persons who are stealing funds from bank accounts often have to act quickly to transfer the money elsewhere, before the customer or banking institution detects or is able to respond to the fraud.

9. At approximately 19:08 UTC, Person A provided detailed information for the Destination Bank Account, including the accountholder name and address, bank name, bank address, and bank account number. The accountholder and bank address were both located in Hong Kong. Person A stated "got it," and a short while later, at approximately 19:20 UTC, wrote, "f---ing did it." BOIKO replied, "good." Person A added, "I'll let you know when they approve."

10. During the same chat, Person A and BOIKO discussed the amount of money that needed to be transferred and the balance in the victim's bank account. Person A referenced "about 200-300k," which, based on my training and experience, refers to approximately two hundred to three hundred thousand dollars that needed to be transferred. Person A further stated, "I've sent around 300k," to which BOIKO replied, "Wow… that's a lot." Person A also advised, "the balance is only 600 there," which, based on my training and experience, is an estimate of how much money was in the victim's bank account.

11. Bank records obtained from Financial Institution 1 indicate that on or about the same date, March 20, 2017, a wire transfer in the amount of approximately $276,300.00 was initiated from Victim A's bank account and was

requested to be sent to the Destination Bank Account. Victim A's account balance was approximately $659,320. The date, transfer amount, balance amount, and recipient account number involved in the attempted transfer all are consistent with Person A's and BOIKO's conversation. Financial Institution 1 rejected the attempted transfer on suspicion of fraud.

12. On or about March 21, 2017, Person A wrote to BOIKO, "it didn't go through, bro... I forgot to write you right away . . . they are f---ed up there . . . they wanted to send a text message to a home phone number :D." On or about March 23, 2017, BOIKO wrote to Person A, "I already knew it didn't work out."

13. In the same March 23, 2017 conversation, BOIKO wrote, in part, "do you think the credentials are compromised or we can keep using them . . . . I think all credentials are ok . . . the account is alive." Person A wrote, in part, "it won't kill your credentials . . . but the same bank won't work for me because it's on the [Financial Institution 1] blacklist." BOIKO replied, "Ok, I'll give, I have 1 more for you." At the end of the chat, BOIKO told Person A that he would provide him with yet another cash-out account. Based on my training and experience, in this chat, BOIKO and Person A were discussing whether Financial Institution 1's rejection of their attempted transaction would prevent them from continuing to use the Destination Bank Account. They determined that BOIKO would continue to be able to access the Destination Bank Account, but that Person A would not be able to transfer funds there because Financial Institution 1 flagged the account as fraudulent. Based on my training and experience, the chat also demonstrated a clear understanding by BOIKO that the failed March 20, 2017 transaction was fraudulent.

14. On or about March 27, 2017, BOIKO wrote to Person A, "OTRv2," to which Person A replied, "sec . . . not here." As discussed above, based on my training and experience, the reference to "OTR" was an instruction by BOIKO to go "off the record," *i.e.*, to switch to encrypted communications.

15. BOIKO and Person A remained in frequent communication. They exchanged messages, predominantly encrypted messages, on or about the following dates: March 28, 2017; April 18, 2017; April 27, 2017; May 9, 2017; June 28, 2017; June 29, 2017; June 30, 2017; July 9, 2017; July 10, 2017; July 11, 2017; July 12, 2017; August 3, 2017; August 9, 2017; August 11, 2017; August 14, 2017; August 15, 2017; August 22, 2017; August 23, 2017; September 11, 2017; and September 12, 2017.

16. On or about May 29, 2017, an unauthorized account user logged into Victim B's online banking account and redeemed Victim B's customer loyalty points. There is probable cause to believe that Person A perpetrated this attack because on or about December 23, 2016, Victim B was previously targeted by a "flooding" attack, during which an unauthorized digital wire of approximately $184,290 was initiated from Victim B's bank account. On or about the same date, Person A sent an online message to another person containing Victim B's business address in Secaucus, New Jersey. Person A further referenced

"184290$" which corresponds to the amount of the fraudulent wire. The May 29, 2017 intrusion was perpetrated in a similar manner, *i.e.*, another flood attack. The victim reported that he received thousands of new emails on his work email address (the same email address that had been flooded in December 2016), and that someone logged into his bank account and withdrew 79,000 corporate points. Furthermore, in chats in January and February 2017, Person A discussed the obtaining and transfer of corporate "points," such as hotel reward points and frequent flyer miles, associated with compromised accounts, which was consistent with the redemption of Victim B's customer loyalty points.

17. On or about June 27, 2017, BOIKO provided Person A with a virtual currency address. From in or about October 2014 until in or about October 2019, that virtual currency address moved over 1,200 bitcoin (which, at the time of the deposits, were worth over approximately $6,500,000).

18. On or about July 5, 2017, Person A had a Jabber chat with an associate. Person A referenced the name of Victim C, as well as the name of its president. The associate responded, in part, "where do you flood phones, on just-kill.cc."[3] Person A responded, "yes."

19. On or about the same date, July 5, 2017, the president of Victim C reported an unauthorized wire of approximately $219,785.00 from its business bank account to a bank account in Hong Kong.

20. Finally, BOIKO's Instagram and Apple iCloud accounts include photographs of him with substantial sums of U.S. and foreign currencies dating back as far as 2015. Based on my training and experience, the unexplained wealth depicted in the photographs is consistent with illegal money laundering. Furthermore, a photograph posted to BOIKO's Instagram account on or about August 25, 2015, shows a large stack of Chinese Yuan on a table, next to a sign that reads, in part, "Maksim" (BOIKO's first name), which is consistent with BOIKO laundering money through Chinese bank accounts, as reviewed above.

21. Law enforcement has determined that the chats reviewed above were, in fact, attributable to BOIKO.

a. A search warrant subsequently executed on an email account associated with BOIKO revealed that he possessed a financial transaction record related to the Destination Bank Account, which confirms that he was in control of that account.

b. The search further revealed that BOIKO was in receipt of a registration confirmation for an online account in the name "Gangass."

[3] Just-kill.cc is a phone and email flooding service used to perpetrate denial of service attacks to victims during fraudulent transfers.

c. Additionally, the investigation revealed that a BTC-e[4] account was registered under the name "Maksim Boiko," the username "gangass," and the email address "**plinofficial**@me.com." The data from BTC-e showed that BOIKO's account had received $387,964 worth of deposits and had withdrawn approximately 136 Bitcoin. Records provided by Google showed that an email address with the same account name, **plinofficial**@gmail.com, was registered in the name Maxim BOIKO. Furthermore, a screenshot sent between BOIKO's phone number (ending in -0504) and another person showed a login to a website with the username "gangass." Google records also showed that a Facebook account registered under the email account "plinofficial@gmail.com" was registered in the name Maxim BOIKO.

d. Finally, a search of an iCloud account associated with BOIKO revealed that BOIKO was "friends" with Individual 1, i.e., the person who introduced BOIKO to Person A.

CONCLUSION

For the foregoing reasons, there is probable cause to believe that BOIKO engaged in the offense of Money Laundering Conspiracy, contrary to Title 18, United States Code, Section 1956(a)(1)(B)(i), in violation of Title 18, United States Code, 1956(h).

[4] BTC-e was a virtual currency exchange website that was seized by law enforcement in 2017 in connection with the website's involvement in the exchange of criminally-derived funds.